- whoami : cmd command to show Device Name and Logged-In Local User Name.

How to Speed Up a Windows 10/11 Computer:
Go To Run and Type:
1st: %temp% (then Delete all the files you can)
2nd: %AppData%\Microsoft\Windows\Recent\AutomaticDestinations (then Delete all the files you can)
3rd: Go To C:\Windows\Prefetch (then Delete all the files you can)
4th: Then Delete Browser cookies and temp Files

Corrupt System File Fix:

Run 1st:
dism.exe /online /cleanup-image /scanhealth
Run 2nd:
dism.exe /online /cleanup-image /restorehealth
Run 3rd:
dism.exe /online /cleanup-image /startcomponentcleanup
Run 4th
sfc /scannow
- Next: Restart the PC and see if the problem is resolved.

- If Not -
- chkdsk /f /r : checks the hard disk for errors (Schedules to Run at Next BootUp)

Other Commands:

- driverquery : shows File System/Kernel hardware drivers/common drivers.
- bcdedit : shows the windows Boot configuration. (Make .txt copy / Store on Other Drive)

To View All Installed Apps:
Power Shell: Get-ProvisionedAppXPackage -Online|Select DisplayName

If cannot open .txt / .jpg / mp4 / etc. trying to use windows Apps:
- Re-Installs and Re-Registeres All Built-In Windows Apps.
Power Shell: Get-AppxPackage -allusers | foreach {Add-AppxPackage -register "$($_.InstallLocation)\appxmanifest.xml" -DisableDevelopmentMode}
(Restart-System)

OS Key Data Commands:

- slmgr /xpr : shows windows key expired: permentaly activated, or 180 days (minuites)

- slmgr /dli : will show windows Key type: Volume/MAK/KMS, OEM, Retail

- slmgr /ipk xxxxx – xxxxx – xxxxx – xxxxx – xxxxx : to change Key - Use dashes -

- slmgr /ato : to Activate

- slmgr /rearm : rearm Key Time Length

- Find OS Key: Type: powershell "(Get-WmiObject -query 'select * from SoftwareLicensingService').OA3xOriginalProductKey"

If you get a message stating Windows is not Genuine please open cmd.exe as administrator and type "slmgr /upk" and hit enter. Then try to activate again. This will remove old key.

Group Policy Management Console: type: gpedit in RUN box or gpmc.msc

secpol.msc - Local Security Policy Editor
gpedit.msc - Local Group Policy Editor
mmc - Add Tool Snap-In Utility

Port Commands:

1. -Loop-Back Local Test = ping 127.0.0.1 - or - ping Localhost -

2. Ping: ping IP Address - 1st
    Ping: ping a Domain-Name URL - 2nd
    - if the Domain-Name URL Ping Failed = DNS problem
    - ping IP Address again to double Verify = DNS problem

3. To See if a Port is open: PowerShell
    $ Test-NetConnection 192.168.1.26 -p 80
    $ Test-NetConnection Google.com -p 80

4. To check IP/URL conductivity/speed of a connection
    tracert -d google.com:
    tracert -d google.com: (Again to compare)

5. arp -a / (Shows IP, MAC and static or Dynamic)

6. ipconfig /all: To see IP, Ethernet and Wireless connection Info.

7. If you find your computer stuck with an IPv4 169.254.x.x IP address, it could

generally mean either of the following:
    - The DHCP server is temporarily unavailable.
    - The computer is not connected properly to the network.
    - The computer is not authorized to connect to the network.

    Options:
    - Disable all of the NIC's you are NOT using.
    - ipconfig /release
    - ipconfig /renew
    - ipconfig /flushdns
    - OR -
    - Open a CMD (ADMIN) prompt and run: netsh int ip reset
    *** You may need to reboot the server to clear the caches and have the change take hold ***

8. nslookup - to see FWD DNS type: nslookup google.com convert URL to an IP address.
                to see REV DNS type: nslookup (googles IP Address) converts IP Address to URL.

9. netstat -b: shows the .exe file that is associated with a Local and Foreign IP Address.

10. netstat -ano: shows Local and Remote open ports, Port State and PID's.

11. netstat -an | find ":80" (Will show Hidden connections)

12. netstat -nap: most effective command line to show an active infection.

13. netstat -rn: Internal Route table